

## DORA: Third Party Management

### SERVICE BENEFITS

- ✓ Expert reviews from DORA specialists who understand the intricacies of the legislation.
- ✓ Objective and impartial third party assessments
- ✓ You'll receive a prioritised action plan for achieving full DORA compliance.
- ✓ Tailored, actionable recommendations for risk mitigation
- ✓ Gain visibility into extended cyber risk exposure

### ACHIEVING THIRD PARTY RISK MANAGEMENT

The Digital Operational Resilience Act (DORA) is set to reshape the financial sector's approach to cybersecurity, and third party risk management is a critical compliance area within the Act. A worrying 50% of organisations don't monitor third parties with access to sensitive and confidential information (Ponemon Institute). Financial institutions now are required to ensure their ICT third party providers meet the stringent DORA requirements.

Razorthorn's DORA Third Party Risk Management service is tailored to help financial institutions navigate this complex aspect of DORA compliance. Our expert team specialises in assessing, managing and mitigating risks associated with your external partners, vendors and suppliers.

We understand that each financial institution has unique needs and challenges. Our service is designed to provide you with a clear understanding of your current third party risk landscape and guide you towards full DORA compliance in this crucial area.

### THIRD PARTY RISK MANAGEMENT: THE RAZORTHORN APPROACH

#### Risk Assessment and Classification

Firstly, we will identify and classify functions that are outsourced to third party providers and assess the potential impact of these services on your operational resilience. We will also evaluate the concentration risk, particularly for cloud service providers. Based on DORA criteria, each third party relationship will be assigned a risk level, in order to guide subsequent management actions.

#### Due Diligence and Contractual Arrangements

Next we will conduct comprehensive due diligence on potential third party providers, with a particular emphasis on their ICT risk management practices. It's crucial to ensure that contractual arrangements include provisions for security measures, access and audit rights, data protection and privacy, service level agreements (SLAs) and business continuity and exit strategies. These elements are essential for maintaining compliance with DORA regulations and protecting your interests.

#### Ongoing Monitoring and Testing

You will be required to implement a third party risk management programme to remain DORA compliant. Razorthorn has partnerships with multiple industry leading third party risk monitoring solution providers and can work with you to select the best option for your requirements. Alternatively, Razorthorn also offers a fully managed third party risk monitoring service.

#### Reporting and Remediation

You will receive a comprehensive report detailing the findings and potential risks, categorised by priority and with actionable recommendations for addressing any identified vulnerabilities. Debriefing sessions will be arranged to discuss results and plan improvements. As required by DORA, significant findings and risk changes must be reported to senior management and regulatory authorities. This step ensures that all parties are informed of the current risk landscape and that necessary improvements are made.

